UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,164	01/14/2000	Daniel Jay Thomsen	105.174US1	8029

21186 7590 03/13/2007

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/483,164	THOMSEN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *14-31 and 33-35* is/are allowed.

6)☒ Claim(s) *1-11,13 and 32* is/are rejected.

7)☒ Claim(s) *12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 1/12/2007 was received and considered.

2. Claims 1-35 are pending.

Response to Arguments

3. Based on the affidavits submitted and applicant's amendments, all prior rejections except the rejections under 35 U.S.C. §102 and §103 are withdrawn.

4. Applicant's response (§3) argues that Applicant cannot find in Sandhu "encapsulating security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key for each security mechanism". Sandhu discloses the following concepts: (1) Permissions are encapsulated into abilities (which can contain other abilities), and (2) abilities are assigned, with users, to roles (which can contain other roles). As Applicant describes, the present invention defines a security mechanism as something that "encapsulates security mechanism application specific information". Sandhu defines a permission as "an approval of a particular mode of access to one or more objects". Therefore, Sandhu discloses security mechanism application specific information because the permissions are application specific (they define precisely an object and an approval for accessing that object in an application) and they are security mechanisms because they define access rights. Further, these are encapsulated to form a key (ability). It is noted that the instant specification provides no clear definition of the limitations "key", "security mechanism" or "semantic layer". These terms are only defined by example in the specification according to their utility; it is argued that Sandhu describes the same utility.

5. Applicant's response (§3) argues that Sandhu does not describe encapsulation, but rather describes a collection. Applicant further alleges that the Office Action reads UP-roles onto the semantic layers of the claims, but does not show that the UP-role of Sandhu does not teach or suggest the flexibility of passing the key chain keys to another semantic layer. However, Sandhu discloses permissions being combined into abilities (keys) and abilities combined with other abilities for form new "broader" abilities (key chains) and encapsulating key chains (again, an abilities) as keys (another ability) and passing the key chain keys (abilities) to another semantic layer (UP-roles) (p. 122, §5). Because UP-roles can contain other UP-roles (UP-roles), there exists another semantic layer where UP-roles are encapsulated into a "broader" UP-role and exported (i.e. a first semantic layer containing UP-roles and a second semantic layer containing combined and encapsulated UP-roles from the first semantic layer) (p. 122, §5). Applicant argues that because Sandhu describes "abilities" as roles and the instant specification describes that "Keys are not capabilities. A key is an abstract representation of some rights, independent of the implementation mechanism, and a capability is data that states the bearer has the rights defined in the capability", that the "abilities" in Sandhu cannot read on the keys recited in the claims. However, as Applicant is relying on an exclusionary definition (i.e. the specification's definition that Keys are not capabilities), Sandhu's abilities must match explicitly Applicant's definition of a capability. However, the abilities (despite Sandhu referring to them as "roles") are not assigned to a user until a UP-role designation (see p. 122, §5.1). Therefore, Sandhu's abilities do not meet the definition of Applicant's capability and therefore this argument is not persuasive.

6. Applicant's response (§3, p. 13) argues that semantic layers are closely tied to static application descriptions. However, this definition is not concrete enough to exclude the Examiner's assertion that a UP-role in Sandhu reads on the semantic layer. Applicant's response further argues that UP-role cannot read on the semantic layer because adding a semantic layer to a role hierarchy does not increase the depth of the hierarchy. However, this is not a definition that clearly describes the metes and bounds of the term "semantic layer". At best, this citation is describing how Applicant's concept of a semantic layer is interacting with a standard role hierarchy. Further, Sandhu does not disclose that only one UP-role can exist and therefore, the addition of another UP-role would not add depth to an existing UP-role if the two were not encapsulated together (i.e. if UP-role1 and UP-role2 were separate groupings for separate purposes).

7. Applicant's response (p. 13, §103 Rejections) argues that the claims are allowable based on the insufficiency of the Sandhu reference. However, as described above, the rejections based on Sandhu are maintained.

8. Applicant's response (p. 14) argues a lack of motivation to combine Sandhu and Crall. However, Crall teaches a concept notoriously well known in the art of computers – graphical user interfaces. As Crall teaches, an administrator can define a security policy using a graphical user interface to manage a large quantity of users (see rejection). One having ordinary skill in the art could have and would have turned to Crall to realize the benefits of graphically administering the invention of Sandhu for the added benefits of scalability, as taught by Crall.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

10. Claims 1-4 & 32 rejected under 35 U.S.C. 102(a) as being anticipated by "The ARBAC97 Model for Role-Based Administration of Roles" by Sandhu et al. (**Sandhu**).

Regarding claim 1, 3 & 32, Sandhu discloses encapsulating security mechanism application specific information/permissions for each security mechanism/permission (p. 122, §5), wherein encapsulating includes forming a key/ability for each security mechanism/permission, combining keys/abilities to form key chains/abilities, encapsulating key chains/abilities as keys/abilities (p. 122, §5) and passing the key chain keys/abilities to another semantic layer/UP-Roles (p. 122, §5), defining the security policy/UP-Roles (p. 122, §5), wherein defining includes forming key chains from keys/abilities and associating users with key chains/abilities (p. 122, §5), translating the security policy/UP-Roles and exporting the translated security policy to the security mechanisms, and enforcing the security policy via the security mechanisms (p. 107, ¶5 & Fig. 1).

Regarding claim 2, Sandhu discloses distributed computer networks/enterprise-wide systems (p. 106, ¶4).

Regarding claim 4, Sandhu discloses UP-Roles, containing both abstracted abilities and permissions (p. 122, §5). If a new role is to be created, the next layer (abilities/users) is drilled to/accessed to combine the necessary elements.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 5-11 & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sandhu**, as applied to claim 1 above, in further view of "Issues in the Design of Secure Authorization Service for Distributed Applications" by Varadharajan, Pato and Crall (**Crall**).

Regarding claim 5, Sandhu discloses a system, as described above, but lacks a graphical user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claim 6-8, Sandhu discloses a plurality of security mechanisms/permissions, a plurality of semantic layers (UP-Roles, abilities, permissions) (p. 122, §5), wherein the first semantic layer combines keys/abilities, wherein each key encapsulates security mechanism application specific information for a security mechanism (permissions for resources) (p. 122, §5), wherein in multiple layers, keys are combined into key chains and exported to another semantic layer (permissions combined into abilities, abilities combined into additional abilities,

combination abilities combined into UP-Roles). Sandhu lacks an explicit translator for translating the security policy to the security mechanisms and lacks a user interface. However, Crall discloses an "Authorization Server", which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a user interface. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu's invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1).

Regarding claim 9, Sandhu discloses the semantic layers (role hierarchy) organized in a POSET/partial order to facilitate inheritance.

Regarding claim 10, Sandhu discloses that new key chains/abilities can be formed by any combinations of abilities and permissions (p. 122, §5), but lacks a user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have

been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claims 11 & 13, Sandhu discloses a model comprising one or more semantic layers/roles for defining different security policies (p. 122, §5) and constraints (p. 108, ¶1) for each type of user, but lacks a tool for manipulating the model and lacks a translator for translating security policies from the model to security mechanisms in one or more computer resources. However, Crall discloses an "Authorization Server", which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a tool for manipulating the model. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu's invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1). As modified, Sandhu discloses enabling an administrator to encapsulate security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key/permission for each security mechanism/permission, combine keys to form key chains/abilities, encapsulate key chains/abilities as keys/abilities within two or more semantic layers (abilities, UP-roles), pass the key chain keys/abilities to other semantic layers (abilities->abilities, abilities->UP-roles, UP-

roles->UP-roles), form user key chains/UP-roles from the key chain keys, and associate users with user key chains (UP-roles designated) (p. 122).

Allowable Subject Matter

13. Claim14-31 & 33-35 are allowed.

14. Claim 12 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. The following is a statement of reasons for the indication of allowable subject matter:

a. Regarding claim 12, the prior art of record fails to teach or disclose, alone or in combination, a static application policy layer, two or more semantic policy layers, and a dynamic local policy layer, in combination with the other elements of the claim.

b. Regarding claim 14, the prior art of record fails to teach or disclose, either alone or in combination, an application policy layer, a first semantic policy layer, a second semantic policy layer and a local policy layer, in combination with the other elements of the claim.

c. Regarding claim 22, the prior art of record fails to teach or disclose, alone or in combination, a static application policy layer, a semantic policy layer and a dynamic local policy layer, in combination with the other elements of the claim.

d. Regarding claim 31, the prior art of record fails to teach or disclose, alone or in combination, a static application policy layer, a semantic policy layer and a dynamic local policy layer, in combination with the other elements of the claim.

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
PRIMARY EXAMINER

MJS

March 6, 2007